

CLAIMS

1-35 (Cancelled)

36. (Original) Computer software operable to provide protection for a second item of computer software, the protection software comprising security means operable to authorise execution of the protected software in response to successful completion of one or more security checks, and having at least one block of executable code which is stored in non-executable form and which requires execution to authorise execution of the protected software, and the protection software further comprising conversion means operable to convert the said block of code to an executable form by means of an algorithm which requires at least one conversion key, the conversion means being further operable to derive a conversion key, for use in the algorithm, by reference to a target block of code in executable or non-executable form, whereby an appropriate conversion key will be derived only if the target block is unmodified.

37. (Original) A computer memory device containing computer software in accordance with claim 36.

38. (Original) A computer system containing an item of computer software protected by means of computer software in accordance with claim 36.

39. (Cancelled)

40. (Previously Presented) A digital data arrangement comprising protected code and security code, wherein the protected code comprises incomplete executable code, the executable code including one or more call instructions to the security code, and the security code, when executed, replaces a respective call instruction with executable code such that the executable code of the protected code is completed upon execution of all call instructions.

41. (Previously Presented) The arrangement of claim 40, wherein the security code, when executed, is operable to detect corruption of the protected code.

42. (Previously Presented) The arrangement of claim 41, wherein the security code is operable to delete the protected code in the event that any corruption is detected.

43. (Previously Presented) The arrangement of claim 40, wherein the protected code comprises encrypted code associated with each call instruction and the security code, upon execution by a call instruction, is operable to decrypt the associated encrypted code and to replace the call instruction and encrypted code with corresponding decrypted code.

44. (Previously Presented) The arrangement of claim 40, wherein the security code is embedded within the protected code.

45. (Previously Presented) The arrangement of claim 44, wherein the security code is embedded at locations which are unused by the protected code.

46. (Previously Presented) The arrangement of claim 45, wherein at least one embedding location is identified when the protected code is executed, the security means is written to the embedding location.

47. (Previously Presented) The arrangement of claim 46, wherein an embedding location is identified by decompiling the protected code, and analyzing the decompiled code.

48. (Previously Presented) The arrangement of claim 40, the arrangement further comprising relocation code operable to change the location of the security code and to modify the call instruction to refer to the new location.

49. (Previously Presented) The arrangement of claim 48, wherein the relocation code is contained within the protected code, to operate repeatedly while the protected code is in use.

50. (Previously Presented) The arrangement of claim 40, wherein the protected code is provided in encrypted form, and the arrangement further comprises executable instructions for decryption.

51. (Previously Presented) A digital data arrangement comprising:
protected data provided in encrypted form;
decryption instructions for decrypting the protected data, the decryption instructions being provided in a non-executable form; and
executable conversion code operable to: derive a conversion key from a target block of data of the arrangement; convert the decryption instructions into an executable form by means of an algorithm that employs the conversion key; and execute the decryption instructions to decrypt the protected data, wherein the decryption instructions are converted into an executable form only in the event that the target block of data is unmodified.

52. (Previously Presented) The arrangement of claim 51, wherein the decryption instructions comprise a plurality of blocks of executable code stored in non-executable form, each of which requires execution to decrypt the protected data, and the conversion code is operable to convert each block into an executable form.

53. (Previously Presented) The arrangement of claim 52, wherein conversion of each block is achieved by a respective conversion key derived from a respective target block.

54. (Previously Presented) The arrangement of claim 52, wherein at least one block is operable, upon execution, to convert another block into an executable form for subsequent execution.

55. (Previously Presented) The arrangement of claim 54, wherein each block is operable, upon execution, to convert another block to an executable form for subsequent execution.

56. (Previously Presented) The arrangement of claim 51, wherein the or each target block is contained within the protected data.

57. (Previously Presented) The arrangement of claim 51, wherein the or each target block is contained within the decryption instructions.

58. (Previously Presented) The arrangement of claim 51, wherein the or each algorithm for converting code is a CRC algorithm.

59. (Previously Presented) The arrangement of claim 51, wherein the protected data contains executable code and/or a data file.

60. (Previously Presented) The arrangement of claim 51, comprising processing means operable to execute code, and memory means storing the protected data, decryption instructions and conversion code with a start point at a memory location indicated within the arrangement as the start point for the protected data, whereby the processor means will cause the executable conversion code to be executed when seeking to access the protected data.

61. (Previously Presented) A digital data arrangement comprising executable code executable to create protected data, wherein the protected data contains at least one executable instruction which contains a plurality of steps, the steps being executable in more than one order to implement the instruction, and the executable code being operable to create the protected data by creating the steps in an order which changes on each execution of the executable code.

62. (Previously Presented) The arrangement of claim 61, wherein the order of the steps is chosen substantially at random on each execution.

63. (Previously Presented) The arrangement of claim 61, wherein the steps include at least one step which initiates operation of security means operable to detect corruption of the protected data.

64. (Previously Presented) The arrangement of claim 61, wherein the executable code is executable to create the steps on each occasion that the executable instruction is to be executed.

65. (Previously Presented) A digital data arrangement comprising executable code executable to create a first part of protected code and to execute the first part of protected code, and to subsequently create a second part of protected code and to execute the second part of protected code, wherein the first part of protected code is corrupted upon creation of the second part of protected code.

66. (Previously Presented) The arrangement of claim 65, wherein each part corresponds to a complete executable routine within the protected code.

67. (Previously Presented) The arrangement of claim 65, wherein the executable code is executable to create corrupt data in addition to each part of protected code.

68. (Previously Presented) A computer system comprising memory means containing a digital protection arrangement according to claim 40.

69. (Previously Presented) A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 40.

70. (Previously Presented) Computer software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 40.

71. (Previously Presented) A digital data arrangement comprising protected code, security code and relocation code, wherein:

the protected code comprises at least one call instruction to the security code;

the security code, when executed, detects corruption of the protected code and executes the relocation code in the event that no corruption is detected; and

the relocation code, when executed, changes the location of the security code and modifies the call instruction to refer to the new location.

72. (Previously Presented) The arrangement of claim 71, wherein:

the protected code comprises a plurality of call instructions to the security code;

the security code, when called by a call instruction, detects corruption of the protected code and, in the event that no corruption is detected, replaces the call instruction with executable code and executes the relocation code; and

the relocation code, when executed, changes the location of the security code and modifies the remaining call instructions to refer to the new location.

73. (Previously Presented) A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 71.

74. (Previously Presented) A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 51.

75. (Previously Presented) A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 61.

76. (Previously Presented) A data carrier containing software which, when installed on a computer system, is operable as a digital data protection arrangement in accordance with claim 65.